

# How far should we let the law follow digital footprints?

**Canadians sent 60 billion text messages last year - a stunning trove of potentially incriminating information. Sometimes it can be used as evidence, sometimes not. Which is why legal experts can't wait for the Supreme Court to set some digital ground rules**

A member of the British Columbia Supreme Court rules that 165 incriminating e-mail messages on a cellphone can be used to prosecute three men in a cocaine conspiracy trial. In Ontario, a judge leans in a different direction, rejecting cellphone evidence in a murder case because police lacked a proper search warrant.

From east to west, and from judge to judge, the struggle to make old privacy laws fit modern-day scenarios is growing more intense. It was never easy for judges to delineate the murky line that separates investigative necessity from personal privacy, but in an era of smartphones, computers and instant messaging, the exercise is fraught with uncertainty.

The result is that the Supreme Court of Canada is bracing for a wave of appeals that will effectively rewrite the rules on privacy and electronic evidence. Its challenge will be to draw a clear line between the right to privacy and the need for law-enforcement officials to mine the memories of cellphones, global-positioning devices and an ever-growing list of new gadgets.

"Rules made back when we talked about kings and castles do not work when we are talking about mobile devices and information technology," says Toronto lawyer Scott Hutchinson, an expert in search and seizure.

Can investigators searching a laptop for signs of fraud change their focus after stumbling upon child pornography? Do computer technicians become agents of the state the moment they come across evidence of crime? Can Internet service providers be recruited by police to filter and reroute text messages?

"The expectation of privacy in a computer is very high," defence lawyer Alan Gold says. "I would rather burn my computer than let anyone get at it. It has the complete record of my life. It is a life in a box. I think a computer has an even higher expectation of privacy than a home."

The parade of challenging cases is mounting. For example, prosecutors in a murder trial under way in Kingston, Ont., concluded that the suspects had used Google to locate bodies of water to conceal evidence of the crime. The search commands they allegedly typed included: "Where to commit a murder," and "Can a prisoner have control over his real estate?"

As for the regional rift in jurisprudence, judges in western Canada have tended to give police considerably more leeway to search electronic devices than their more privacy-oriented colleagues in the east.

"Hopefully, the divergence between the west and the east will be resolved by the Supreme Court," Alberta prosecutor Steven Johnston told a York University evidence conference recently. "I deal with a lot of files that often cross provincial borders. It causes us no end of consternation trying to figure out which law we are going to go under. Will it be Ontario search law? Will it be B.C. search law, which is markedly different?"

Close to 60 billion text messages were sent in Canada last year - a figure that hints at the stunning trove of intimate information contained in devices like cellphones. Increasingly, the courts are relying on experts to help them weigh the merits of allowing or excluding electronic evidence.

One of those experts - Daniel Embury, head of an RCMP forensic-science unit in Ottawa - works in a small, cluttered lab where he and the five technicians under his command are deluged by a blizzard of devices to be disassembled and analyzed.

Frequently they have to crack into outdated relics, devices that have been saturated with blood, beaten with hammers or run through cellphone "shredders" in sophisticated attempts to obliterate their contents. "Anything that was designed by a person can be reverse-engineered," Mr. Embury says.

His team was charged with obtaining data from cellphones destroyed by a group of illegal Tamil refugees as their vessel neared the B.C. coast in 2010, and helping British police obtain encrypted information on BlackBerry devices as part of an investigation into cricket games that had been fixed.

But the extraction is only half the battle. Prosecutors must then persuade judges to accept information that was intended to remain private. If judges lean too far in the direction of law enforcement, Orwellian scenarios could result.

Contracts between Internet servers and customers have become a major threat to privacy, Mr. Gold says, adding that companies are often contractually permitted to give police private information that can help investigators circumvent search-and-seizure laws. "Police get the information through the back door," he says. "They don't need a search warrant; they just need a sympathetic ISP."

Another specialist in the field, lawyer Scott Fenton, says courts look at several key criteria that include: the nature of the subject matter; whether an accused person had control of the data and could regulate access to it; what his expectation of privacy was, and whether that expectation accords with what a reasonable person would think. The results vary widely, both across trials and sometimes even within a single case.

Ontario Crown counsel Michal Fairburn told the York University conference that an Ontario judge in one recent case barred the use of incriminating material found on a defendant's BlackBerry but ruled in favour of the Crown using evidence derived from a strip search of the man.

While most people would find a strip search considerably more intrusive than a search of their cellphone, Ms. Fairburn said, the judge went in the opposite direction: "Therein, lies the problem with the way the law has evolved," she explained.

Mr. Gold says future search warrants are likely to carry strict conditions as to what police can or cannot view during a digital search: "Police searches have to be transparently recorded so that the subject of the search can ensure his constitutional rights were adhered to."

Some U.S. courts, he explains, have gone so far as to order the use of search techniques that take police just to computer files that are specified in their warrants.

And what is to stop them from going any farther? The same techniques make it possible to trace the electronic footprints that the investigators leave behind.